STATEWIDE INFORMATION SYSTEMS POLICY

Statewide Policy: Remote Access for Employees and Contractors

Product ID: ENT-SEC-130

Effective Date: November 20, 2001

Approved: Steve Bender, Acting Director, Department of Administration

Replaces & Supercedes: This policy supercedes any prior enterprise policies for establishing and implementing information technology (IT) policies and standards.

I. Authorizations, Roles, & Responsibilities

Pursuant to the Montana Information Technology Act ("MITA") (Title 2, Chapter 17, Part 5 of the Montana Code Annotated ("MCA"), it is the policy of the state that information technology be used to improve the quality of life of Montana citizens, and that such improvement is to be realized by protecting individual privacy and the privacy of the information contained within the state's information technology systems. §2-17-505(1), MCA. It is also the policy of the state that the development of information technology resources be conducted in an organized, deliberative, and cost-effective manner, which necessitates the development of statewide information technology policies, standards, procedures, and guidelines applicable to all state agencies and others using the state network. It is also anticipated that State information technology systems will be developed in cooperation with the federal government and local governments with the objective of providing seamless access to information and services to the greatest degree possible. §2-17-505(2), MCA.

Department of Administration: Under MITA, the Department of Administration ("DOA") is responsible for carrying out the planning and program responsibilities for information technology for state government (except the national guard), including for establishing and enforcing a state strategic information technology plan and establishing and enforcing statewide information technology policies and standards. DOA is responsible for implementing MITA and all other laws for the use of information technology in state government. The director of DOA has appointed the chief information officer to assist in carrying out the department's information technology duties. §2-17-512, MCA.

Department Heads: Each department head is responsible for ensuring an adequate level of security for all data within their department. §2-15-114, MCA.

II. Policy - Requirements

A. Scope

This policy applies to all state employees and state contractors accessing a state computer or system that resides on the inside of the state's Internet firewall, including all state agencies as well as local government entities. This policy does not apply to colleges and universities, the Commissioner of Higher Education Office, or public access computers in libraries.

B. Purpose

The Summit Net Executive Council has the responsibility to ensure that the state's information technology resources are used in the most secure manner. The following policy relates to the access to state information technology resources through remote access for employees as well as contractors with the State of Montana. This policy outlines the requirements established for remote access to state computing resources and the appropriate use of this access.

C. Requirements

ITSD will provide a secured connection via dedicated, dialup or Internet connection, to access all state information technology resources. Agencies are to use only this connection for remote access into the state's information technology resources. Any remote access mechanisms used prior to this policy will be migrated to the connection provided by ITSD by **September 1, 2002**.

The appropriate agency administrator must provide requests for remote access for each employee or contractor in writing to ITSD. ITSD will provide the agency with the procedures to be used so that their employee or contractor can connect to the state network.

Remote access users are obligated to abide by all computing policies of the state and the agency. Access will be granted for legitimate business uses of the State of Montana and not for personal use. Access to the state's information technology resources by unauthorized remote users will be considered a violation of state policy.

ITSD may grant exceptions to this policy to an agency if the secured remote service provided does not meet Federal or some other contract requirements. A full security review of the agency's proposed exception will be conducted by ITSD to ensure that the request and proposed solution meet enterprise security requirements.

Background - History on the creation of or changes to this policy

The Computing Technology Services Bureau of the Information Technology Services Division created this policy.

This policy was distributed to the SummitNet Executive Council for comment prior to adoption.

D. Guidelines - Recommendations, Not Requirements

There are no guidelines for this policy.

E. Change Control and Exceptions

Policy changes or exceptions are governed by the Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards. Requests for a review or change to this policy are made by submitting an Action Request form. Requests for exceptions are made by submitting an Exception Request form. Changes to policies and standards will be prioritized and acted upon based on impact and need.

III. Close

For questions or comments about this instrument, contact the Information Technology Services Division at ITSD Service Desk, or:

Chief Information Officer
PO Box 200113
Helena, MT 59620-0113
(406) 444-2700
FAX: (406) 444-2701

IV. Cross-Reference Guide

A. State/Federal Laws

- 2-17-505(1) – Policy
- 2-17-514(1) – Enforcement
- §2-17-505(2), MCA
- §2-17-512, MCA
- §2-15-114, MCA
- 2-17-532-534, MCA

B. State Policies (IT Policies, MOM Policies, ARM Policies)

- 2-15-112, MCA
- MOM 1-0250
- MOM 3-0130 Discipline
- MOM 3-0620 (now included in MOM 3-0630)
- Internet Acceptable Use Policy
- SummitNet Acceptable Use Policy
- Transmission Privacy Policy
- User Responsibilities Policy.
- ARM 2.13.101 - 2.13.107 - Regulation of Communication Facilities
- ARM 2.12.206 Establishing Policies, Standards, Procedures and Guidelines.

C. IT Procedures or Guidelines Supporting this Policy

- Policy: Establishing and Implementing Statewide Information Technology Policies and Standards
- Procedure: Establishing and Implementing Statewide Information Technology Policies and Standards

V. Administrative Use

Product ID:	ENT-SEC-130
Proponent:	Steve Bender, Acting Director, Department of Administration
Version:	1.1
Approved Date:	July 15, 2008
Effective Date:	November 20, 2001
Change & Review Contact:	ITSD Service Desk
Review Criteria:	Event Review: Any event affecting this policy may initiate a review. Such events may include a change in statute, key staff changes or a request for review or change.
Scheduled Review Date:	July 1, 2013
Last Review/Revision:	Reviewed July 11, 2008. Non-material changes are necessary.
Change Record:	July 11, 2008 – Non-material changes made: - Standardize instrument format and common components. - Changed to reflect next review date.